UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR. | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/092,277 | 03/06/2002 | Ian Curry | 10500.02.0123 | 7718 |

23418 7590 12/14/2006

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

| EXAMINER | |
|---|---|
| PICH, PONNOREAY | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

DATE MAILED: 12/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/092,277 | CURRY, IAN | |
| | Examiner | Art Unit | |
| | Ponnoreay Pich | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *19 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/19/2006 has been entered.

Claims 1-28 are pending, where claim 28 is newly added. Any well known art statements made in the prior office action not specifically or adequately traversed by applicant are taken as admittance of prior art as per MPEP 2144.03.

### *Response to Arguments*

Applicant's arguments were fully considered, but were not persuasive. Applicant first argues that one of ordinary skill recognizes that the word "software" as used in the specification context does not refer to software per se such as software instructions written on a piece of paper, but instead refers to instructions stored in memory or executing by circuitry such as processing device. In response, the examiner respectfully does not see where applicant is getting the idea that the examiner is interpreting software per se as instructions written on a piece of paper. The examiner is interpreting software per se as the software module or executable itself. For instance, if one were to purchase a CD containing executable modules for installing an operating system onto a computer, the executable modules by themselves are considered software per se. Claims to just the modules (i.e. software per se) would not be

statutory, while claims to the modules in combination with the medium (i.e. the CD) would be statutory or if the software was installed onto a computer, claims to just the software modules installed on the computer would not be statutory, while claims to the installed modules as well as any of the hardware on which the software has been installed would be statutory.

Applicant further argues that as to the network element on page 7 and 8 of the specification, the reference to discrete logic or any suitable combination refers to combination of hardware/software, hardware/firmware or any suitable combination for purpose of operation. In response, applicant is reminded that though the claims are read in light of the specification, limitations from the specification cannot be read into the claim. While it is true that the network element discussed in the specification can contain hardware, i.e. the one or more processing devices discussed in paragraph 19, the components of the network element being claimed does not refer to the hardware discussed in the specification. Claim 18 is the claim to a network element, so claim 18 will be referred to for discussion. In claim 18, means for decrypting refers to the decryptor 24, which paragraph 19 states is a software module. The means for obtaining refers to transceiver 22, which paragraph 19 states may be ... "software", see lines 2-4. The means for encrypting refers to the encryptor 28, which paragraph 19 states is a software module. The means forwarding also refers to the transceiver 22, which as discussed, refers to software. All the components recited for the claimed network element of claim 18 refers to software. Despite the specification disclosing that the network element has hardware, if these hardware components are not claimed, they

cannot be considered. As such, it is interpreted that applicant is only claiming a network element comprising only software components.

Applicant states that new claim 28 indicates one example of means for decrypting, where software may be executing on a microprocessor. The examiner notes that claim 28 recites "at least one processor that includes the means for decrypting, the means for obtaining a corresponding public key and the means for encrypting the secret key". The examiner notes that a processor can refer to either hardware, i.e. microprocessor, or software, i.e. a computer program, see page 872 of attached IEEE document. In referring to "processor" of claim 28 as "microprocessor", applicant is not using a broad enough interpretation of the claim. One skilled should appreciate that a computer program can be composed of several modules, thus the processor of claim 28 will also be interpreted as referring to software, i.e. a computer program.

Applicant requested a definition for what the examiner is using for "software per se". The examiner had explained above that software per se is being interpreted as referring to software modules by themselves without any underlying hardware upon which the modules are stored or upon which they could be executed to run. Applicant states that one of ordinary skill would not understand the disclosure to describe software per se as being able to accomplish any function. The examiner agrees. Software by itself would not be able to accomplish any function, thus is partly the reason why claims to just the software without any hardware is not considered statutory. Microsoft Word is a program that is a means for word processing. However, without

underlying hardware for the program to run on, word processing will not be accomplished. Applicant's specification describes a network element having combination of hardware and software which allows it to accomplish its functionalities. However, applicant's claims in dispute only refers to the software, which would not allow the network element to accomplish any functionality since it needs the underlying hardware to allow to software to function.

As to claim 1, applicant states the key used in Perlman produces not a recipient specific secure secret key, but group specific keys. The examiner respectfully notes that if the secure secret key is specific to the group and the recipient is a member of the group, the secret key is also specific to the recipient. The limitation under contention states "encrypting the decrypted secret key for the at least one intended recipient using a corresponding public key to produce at least one recipient specific secure secret key". The limitation does not prohibit the key from being specific to anyone else other than just one recipient. As long as it is specific to at least one recipient, it is immaterial that it is also specific to other members of a group.

Claims 1-27 were not amended and arguments for these claims have been traversed. The rejections for claims 1-27 are repeated below for record. New rejection for newly added claim 28 is also made below.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 18-19 and 24-28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

**Claim 18:**

Claim 18 refers to a software network element comprising software means. Note that on page 7-8 of the specification, applicant defined a network element such that it "may be an intranet" or it "may be implemented as a server suitably coupled to one or more wide are networks...." However, this language does not exclude the network element being software alone. Software by itself is non-statutory. The examiner respectfully suggests including the limitation of a processing means which refer to the one or more processing devices discussed in paragraph 19 to overcome this rejection. These one or more processing devices are discussed as referring to various hardware or hardware combination.

**Claim 19:**

Claim 19 merely further defines the software network element of claim 18. Nothing statutory was recited.

**Claim 24:**

Claim 24 recites a secure communication system which can be implemented in software alone as the limitations it comprises all read on software elements.

**Claim 28:**

Claim 28 recites at least one processor that includes the means for decrypting, the means, for obtaining a corresponding public key and the means for encrypting the

secret key. These means are software means and as discussed previously, the term "processor" can mean either hardware (microprocessor) or software (computer program), thus claim 28 is not statutory since one can interpret it as referring to only software.

**Claims 25-27:**

Claims 25-27 merely further define the software communication system of claim 24. Nothing statutory was recited.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3-8, 10, 15, 17-20, 22-24, and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Perlman et al (US 6,912,656).

**Claim 1:**

Perlman discloses the limitations of:

1. Receiving encrypted information from a sender for transmission to at least one intended recipient and receiving an encrypted secret key encrypted using a

public key associated with a secure distribution server (Fig 4A-4C; col 5, lines 10-15 and 34-37; col 6, lines 47-65; and col 7, lines 41-59).

2. Decrypting the encrypted secret key to produce a decrypted secret key (Fig 4A-4C and col 7, lines 41-59).
3. Obtaining a corresponding public key of the at least one intended recipient using a corresponding public key to produce at least one recipient specific secure secret key (Fig 4A-4C and col 7, lines 41-59).
4. Forwarding the encrypted information sent by the sender and at least one recipient specific secure secret key for the at least one intended recipient (Fig 4A-4C; col 5, lines 23-37; and col 7, lines 51-59).

**Claim 3:**

Perlman further discloses wherein the step of encrypting the decrypted secret key with a corresponding public key of the at least one intended recipient includes encrypting a copy of the decrypted secret key for each intended recipient with a corresponding recipient public key (Fig 4A-4C). Note the group public key corresponds to each recipient and the private key held by each recipient.

**Claim 4:**

Perlman further discloses encrypting information with the secret key to produce the encrypted information, encrypting the secret key with a public key associated with the secure distribution server to produce the encrypted secret key, and sending the encrypted information and the encrypted secret key to the secure distribution server (Fig 4A-4C; col 5, lines 10-15 and 34-37; col 6, lines 47-65; and col 7, lines 41-59).

**Claim 5:**

Perlman further implicitly discloses wherein encrypting the secret key includes encrypting the secret key using a public key for each of a plurality of secure distribution servers to produce a plurality of secure distribution server specific encrypted secret keys (Fig 4A-4C and col 4, lines 47-51).

**Claim 6:**

The limitation of storing the encrypted information in an encrypted form locally on a device that performed the step of encrypting information with the secret key is inherent to Perlman's invention. To be able to encrypt and then forward the encrypted information to the secure distribution server, the device which performed the encryption process must store the encrypted information locally in memory before being able to send the encrypted information.

**Claim 7:**

Perlman further discloses the step of encrypting the secret key, by a sending device, with a public key associated with at least one of a user of the sending device and the sending device (Fig 4A-4C). Note that the DLE and group server are also sending devices. The recipients are users of the DLE and group server.

**Claim 8:**

Perlman further discloses the step of digitally signing the information using a private signing key associated with at least one of a user of a sending device and the sending device (col 4, lines 52-64 and col 5, lines 58-67).

**Claim 10:**

Perlman further discloses the step of determining, by the secure distribution server, if the encrypted information needs to be sent to other entities, if so, encrypting the decrypted secret key using a public key associated with each of the additional entities (Fig 4A-4C; col 5, lines 10-15 and 34-37; col 6, lines 47-65; and col 7, lines 41-59). Note the other entities read on the additional recipients in the distribution list.

**Claim 15:**

Perlman discloses the limitations of:

1. Receiving, by a secure distribution server, encrypted information from a sender for transmission to a plurality of recipients and an encrypted secret key encrypted using a public key associated with a secure distribution server (Fig 4A-4C; col 5, lines 10-15 and 34-37; col 6, lines 47-65; and col 7, lines 41-59).
2. Decrypting, by the secure distribution server, the encrypted secret key to produce a decrypted secret key (Fig 4A-4C and col 7, lines 41-59).
3. Obtaining, by the secure distribution server, a corresponding public key of the at least one intended recipient using a corresponding public key to produce at least one recipient specific secure secret key (Fig 4A-4C and col 7, lines 41-59).
4. Forwarding, by the secure distribution server, the encrypted information sent by the sender and at least one recipient specific secure secret key for the at least one intended recipient (Fig 4A-4C; col 5, lines 23-37; and col 7, lines 51-59).

**Claim 17:**

Claim 17 recites a limitation substantially similar to what is recited in claim 3 and is rejected for the same reasons.

**Claim 18:**

Claim 18 is directed towards a network work element comprising means for implementing the method of claim 1. Claim 18 is rejected for similar reasons given in claim 1.

**Claim 19:**

Claim 19 recites a limitation substantially similar to what is recited in claim 12 and is rejected for the same reasons given for claim 12 below.

**Claim 20:**

Claim 20 is directed towards a storage medium comprising memory containing executable instructions that when read by one or more processing devices, causes the one or more processing devices to implement the method of claim 1. Note that because Perlman's invention is computer implemented, a memory containing executable instructions that when read by one or more processing devices, cause the one or more processing devices to perform the method of claim 1 is inherent to Perlman's invention. Claim 20 is rejected for the same reasons given in claim 1.

**Claim 22:**

Perlman further inherently discloses memory containing executable instructions that when read by the one or more processing devices causes the one or more processing devices to encrypt a copy of the decrypted secret key for each intended recipient with a corresponding recipient public key (Fig 4A-4C).

**Claim 23:**

Perlman further inherently discloses memory containing executable instructions that when read by the one or more processing devices causes the one or more processing devices to determine if the encrypted information needs to be sent to other entities, if so, encrypting the decrypted secret key using a public key associated with each of the additional entities (Fig 4A-4C).

**Claim 24:**

Perlman discloses the limitations of:

1. At least one sender that encrypts information with a secret key to produce encrypted information, encrypts the secret key with a public key associated with a network element to produce an encrypted secret key, and during an online session, sends the encrypted information and the encrypted secret key to the network elements (Fig 1, item 104 and 4A-4C).
2. At least one intended recipient (Fig 1, items 106 and 108).
3. At least one network element, operatively coupled to the sender and to the at least one intended recipient (Fig 1, items 110, 116, and 114), including means as recited in claim 18.

The means of the at least one network element recited in claim 24 are rejected for the same reasons given in claim 18.

**Claim 26:**

Claim 26 recites the means for performing the limitation of the method recited in claim 12 and is rejected for the same reasons given in claim 12 below.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 9, 12-13, 16, 21, 25-26, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656).

**Claim 2:**

Perlman further discloses determining a plurality of intended recipients and retrieving a corresponding public key of the plurality of intended recipients for encrypting the decrypted secret key (Fig 4A-4C and col 2, lines 22-31).

Note that in Perlman's invention, each of the recipients share one group public key, while holding their own copy of the private key corresponding to that public key. Perlman does not explicitly disclose that each of the plurality of intended recipients have corresponding public **keys**. However, Perlman's invention still reads on the limitation recited in claim 2 because each of the recipient has a copy of the private key, so in that manner each recipient's privately held private key forms a public/private key pair with the public key that was used to encrypt the secret key for secure transmission to the recipients. The limitation as recited in claim 2 does not deviate from the spirit of Perlman's invention.

Further, the examiner notes that recipients with their own public/private key pair were well known at the time the applicant's invention was made. It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to have replaced the group public key in Perlman's invention with a public key from each recipient's public/private key pair and used each recipient's public key to encrypt a copy of the message secret key for secure transmission to each recipient. One of ordinary skill would have been motivated to do so as this would allow the secret key to be sent securely to each recipient without having to place each recipient in a group list first.

**Claim 9:**

Perlman does not disclose the step of receiving the encrypted information and the encrypted secret key and forwarding the encrypted information and the encrypted secret key to the secure distribution server without decrypting the encrypted secret key. However, this limitation reads on forwarding/routing packets by nodes in a network, which was well known and commonly used in networks at the time applicant's invention was made. It would have been obvious to one of ordinary skill in the art to have modified Perlman's invention according to the limitations recited in claim 9. One of ordinary skill would have been motivated to do so as direct connections between a sender and receiver in a network are rare and packets often have to be received and forwarded by other nodes in the network before the packets get to the final destination node.

**Claim 12:**

Perlman further discloses wherein retrieving the corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key includes obtaining the corresponding public keys from at least one of: a certificate retrieval and validation service, an LDAP lookup and a certificate directory lookup (col 7, lines 13-28).

**Claim 13:**

Perlman discloses the steps of: encrypting information with a secret key to produce the encrypted information, encrypting the secret key with a public key associated with the secure distribution server to produce the encrypted secret key, and during an online session, sending the encrypted information and the encrypted secret key to the secure distribution server (Fig 4A-4C).

Perlman does not explicitly disclose the encryption of the information and secret key are done offline. However, the examiner submits that encrypting information and a secret key offline is well known in the art. For example, it is well known that a user can prepare an email message for sending on a laptop when the laptop does not have a network connection, i.e. if the user was on a plane for a business trip. The message is usually prepared to a state where the only thing needed to be able to send the email is a network connection. Later, when the laptop is connected to a network, the message can then be sent. It would have been obvious to have the encryption of the message and key done offline prior to connecting to a network as the encryption process might take a long time and connection charges on the road can be expensive.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Perlman's invention

according to the limitations recited in claim 13. One of ordinary skill would have been motivated to do so as it is common practice to be able to prepare messages offline during business trips and one of ordinary skill would have been motivated to encrypt the message and key offline prior to sending when a computer is online as it would reduce the amount of time the computer has to be connected to a network; this would reduce connection fees where the user is charged by the minute.

**Claim 16:**

Claim 16 recites a limitation substantially similar to what is recited in claim 2 and is rejected for the same reasons.

**Claim 21:**

Claim 21 recites a limitation substantially similar to what was recited in claim 2 and is rejected for the same reasons.

**Claim 25:**

Claim 25 recites a limitation substantially similar to what is recited in claim 13 and is rejected for the same reasons.

**Claim 28:**

As per claim 28, the examiner applies two interpretations to the limitation recited therein—one where processor refers to a software program and a second where processor refers to a microprocessor.

The rejection as per the first interpretation is made in this paragraph. Perlman does explicitly disclose at least one processor that includes the means for decrypting, the means for obtaining a corresponding public key and the means for encrypting the

secret key. However, as discussed in claim 1 and 18, software means to decrypt, obtain, and encrypt were disclosed by Perlman. Further official notice is taken that software programs which were further composed of submodules were well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to have the means for decrypting, obtaining, and encrypting be included as submodules for a larger processor program. One skilled would have been motivated to do so because the choice to have the three means running as separate programs or as part of one larger processing program is an arbitrary engineering design choice.

As for the second interpretation of the limitation, Perlman also does not explicitly disclose at least one (micro)processor that includes the means for decrypting, the means for obtaining a corresponding public key and the means for encrypting the secret key. However, one skilled should appreciate that software modules are executed by microprocessors, thus it would have been obvious to one skilled in the art to have at least one (micro)processor that includes the means recited in claim 28. One skilled would have been motivated to do so because execution of code by a processor is how programs are carried out for a computer.

Claims 11 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) in view of Chen et al (US 5,832,208).

**Claim 11:**

Perlman discloses the steps of: encrypting the decrypted secret key using a public key and sending the encrypted information and the encrypted secret key.

Perlman does not disclose the public key is associated with a content scanning device; the sending is to the content scanning device; receiving a result back from the content scanning device, forwarding the encrypted information based on the result sent by the content scanning device and based on at least one recipient specific secure secret key for at least one intended recipient.

However, Chen discloses a virus scanner, i.e. content scanning device, being implemented on a server (col 5, lines 53-60). Chen discloses that emails sent to the server are scanned for viruses, an alert is generated if a virus is detected, and if possible, the virus is removed from the email attachment (col 5, lines 25-27 and col 7, lines 57-60).

In light of Chen's teachings, it would have been obvious to one of ordinary skill in the art to have combined Perlman and Chen's teachings according to the limitations recited in claim 11. One of ordinary skill would have been motivated to do so as scanning messages for viruses and removing the virus from email messages would prevent the spread of viruses to recipients of the email messages, which would compromise the recipient's system and any network they are attached to.

**Claim 27:**

Claim 27 recites a network element which performs the limitations of the method recited in claim 11 and is rejected for the same reasons given in claim 11.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) in view of Bouchard et al (US 2002/0091928).

**Claim 14:**

Perlman does not disclose sending the encrypted information to a time stamper and receiving a time stamped result prior to forwarding the encrypted information and the at least one recipient specific secure secret key to the at least one corresponding intended recipient.

However, Bouchard discloses time stamping a message by a time stamper prior to forwarding the message to a recipient (p3, paragraph 31, lines 11-15 and Fig 2). In light of Bouchard's teachings it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Perlman's invention according to the limitations recited in claim 14. One of ordinary skill would have been motivated to do so as Bouchard discloses that applying a time stamp to a message allow for an audit log of the message, which is useful in preventing the repudiation of digitally-signed documents/messages (p3, paragraph 28).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100